The number of correctable errors of weight d/2+1 for the 1st-order Reed-Muller code

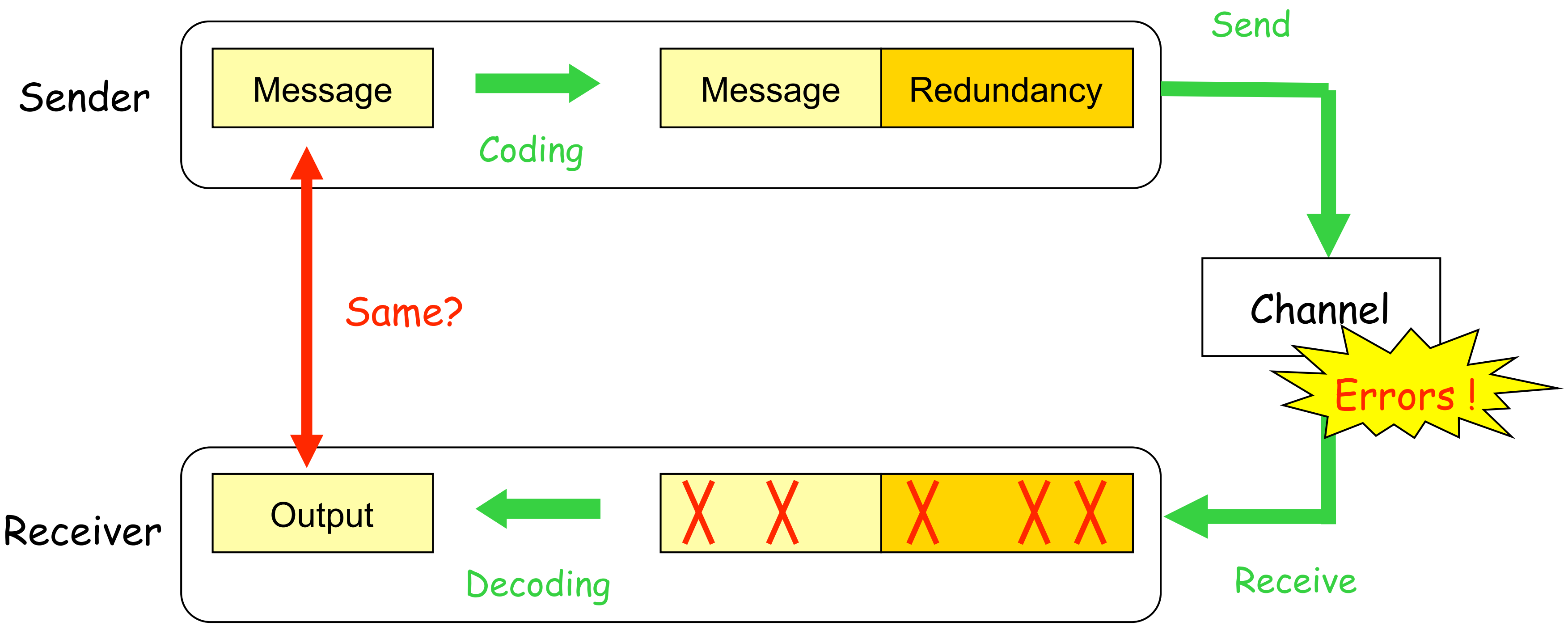
Kenji Yasunaga

Information security engineering laboratory

Osaka University

Error Correcting Codes

- Can correct errors in channels by adding redundancy to message



Error Correction Capability

d : the minimum distance of the code

$w(e)$ = #(corrupted bits in error e)

- If $w(e) < d/2 \Rightarrow$ Always correctable!
  If $w(e) \geq d/2 \Rightarrow$??
  - Analysis for $w(e) \geq d/2$ is a difficult problem

In this work,
we investigate #(correctable errors e for $w(e) \geq d/2$)

Main results

- #(correctable errors of $w(e)=d/2+1$) for the 1st-order Reed-Muller codes is derived
  - Probably the first nontrivial result of the exact number for $w(e)=d/2+1$ for error correcting codes

Main technique

- Monotone error structure
  - Already appeared in [Peterson, Weldon, 1972]
  - But there is only few research using this structure
    - We show the usefulness of this structure

Monotone error structure (1/2)

We introduce covering relation for vectors

$$x \subseteq y \quad \Leftrightarrow \quad x_i \le y_i \text{ for all } i$$

- Example

$$000 \subseteq 001 \subseteq 011 \subseteq 111$$

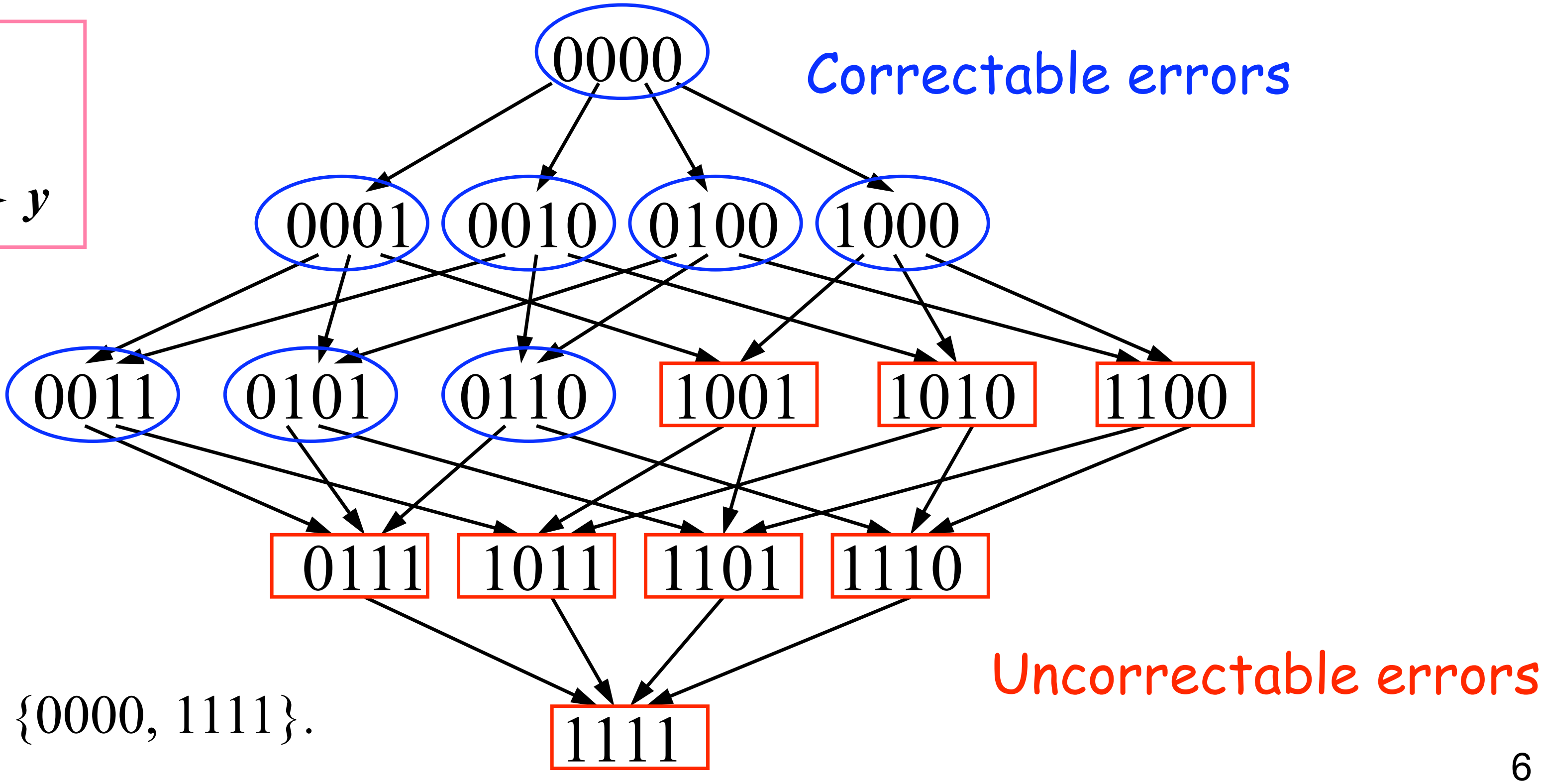
$$0000 \subseteq 0110 \subseteq 1110 \subseteq 1111$$

Monotone error structure (2/2)

x is correctable $\Rightarrow$ all y s.t. $y \subseteq x$ are correctable

x is uncorrectable $\Rightarrow$ all y s.t. $x \subseteq y$ are uncorrectable

$$x \subseteq y \iff x \longrightarrow y$$



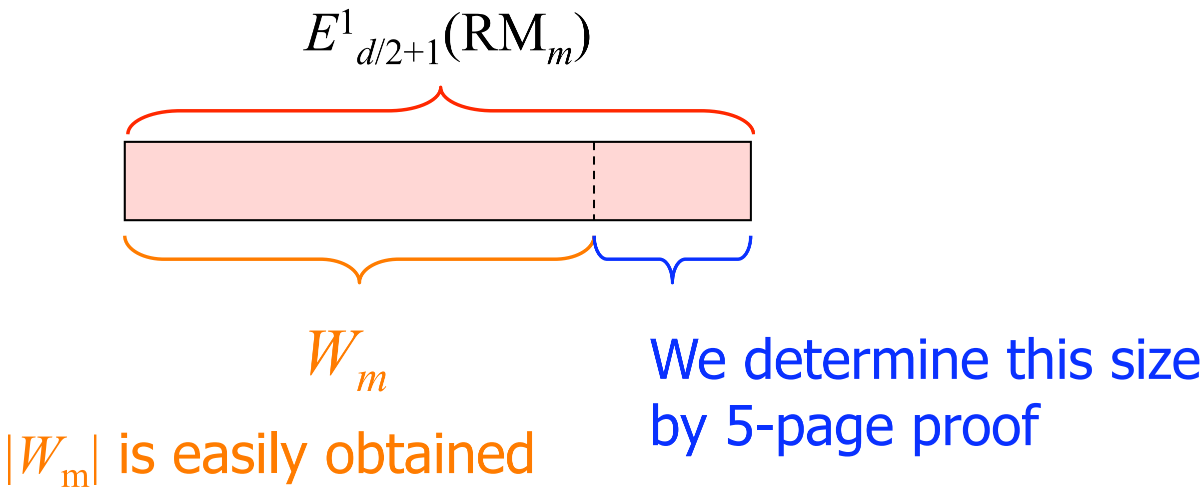
The code is $\{0000, 1111\}$.

The result

- $|\underbrace{E^1_{d/2+1}(\mathrm{RM}_m)}_{\text{Uncorrectable errors}}| = 4(2^m - 1)(2^{m-3} + 1)\binom{2^{m-1}}{2^{m-2}+1} - (4^{m-2} + 3)\binom{2^m}{3}$

$$\underbrace{|E^0_{d/2+1}(\mathrm{RM}_m)|}_{\text{Correctable errors}} + |E^1_{d/2+1}(\mathrm{RM}_m)| = \binom{2^m}{2^{m-2}+1}$$

Very very short proof sketch



- $W_m = \{\, v : v \subseteq c \text{ for } c \in \mathrm{RM}_m \setminus \{0,1\},\ w(v) = d/2+1 \,\}$

$$|W_m| = 2(2^m - 1)\binom{2^m}{2^{m-2}+1}$$